МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

ОДЕСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

КІБЕРБЕЗПЕКА В УКРАЇНІ: ПРАВОВІ ТА ОРГАНІЗАЦІЙНІ ПИТАННЯ

International scientific-practical conference
«Cybersecurity in Ukraine: Legal and Organizational Issues»

Матеріали
Міжнародної науково-практичної конференції
17 листопада 2023 року

Одеса
ОДУВС
2023

Рекомендовано до друку рішенням кафедри кібербезпеки та інформаційного забезпечення
Одеського державного університету внутрішніх справ

Всі матеріали надані в авторській редакції та виражають персональну позицію учасника конференції

Кібербезпека в Україні: правові та організаційні питання: матеріали міжн. наук. практ. конф., м. Одеса, 17 листопада 2023 р. Одеса : ОДУВС, 2023. -- - 168 с.

У збірнику представлено стислий виклад доповідей і повідомлень, поданих на міжнародну науково-практичну конференцію «Кібербезпека в Україні: правові та організаційні питання», яка відбулася на базі кафедри кібербезпеки та інформаційного забезпечення Одеського державного університету внутрішніх справ 17 листопада 2023 року.

У матеріалах конференції приділено увагу актуальним теоретичним та практичним проблемам забезпечення інформаційної безпеки в Україні. Висвітлюється широкий спектр питань, пов’язаних з удосконаленням правового регулювання та адміністративно-правового забезпечення кібербезпеки в Україні. Розглянуто використання інформаційних систем, технологій та інформаційно-аналітична діяльність правоохоронних підрозділів у боротьбі з злочинністю та надано обґрунтовані рекомендації щодо вдосконалення підготовки персоналу для боротьби з кіберзлочинністю в Україні.

Матеріали міжнародної науково-практичної конференції адресовано вченим, працівникам правоохоронних органів, аспірантам (ад’юнктам), здобувачам вищої освіти першого та другого півня освіти.

списання коштів з банківських рахунків за допомогою систем дистанційного банківського обслуговування, заволодіння коштами громадян через інтернет-аукціони, інтернет-магазини, сайти та телекомунікаційні засоби зв'язку, протиправний контент, який пропагує екстремізм, тероризм, наркоманію, культ жорстокості і насильства. Використання інформаційно-комунікаційних технологій може стати головним чинником зміцнення законності, забезпечення обороноздатності країни, соціально-політичної стабільності та розвитку демократичних засад в управлінні державою. Значна роль інформаційного забезпечення у процесі здійснення ефективного управління в Органах національної поліції та функціонування усієї правоохоронної системи підтверджується на практиці боротьби зі злочинністю. Важлива роль системи інформаційного забезпечення управління в правоохоронних органах підтверджується на нормативному рівні, зокрема наказами та розпорядженнями МВС України. Буде доцільним застосовувати якісний та ефективний досвід розвинутих зарубіжних країн, що полягає в реалізації та втіленні корпоративної об'єднаної інформаційної моделі даних для потреб поліції.

Отже, використання інформаційно-комунікаційних технологій в правоохоронних органах є невід'ємною складовою їх діяльності, що забезпечує викриття, припинення, та боротьбу зі злочинністю за допомогою отриманої інформації, а також за допомогою міжнародного досвіду розвинутих країн здобуття доцільних та ефективних технологій у вдосконаленні цілої системи інформаційних технологій. Актуальним є розуміння основних інформаційних систем в правоохоронній діяльності, знання особливостей використання інформаційних систем окремими підрозділами правоохоронних органів, розуміння основ використання та правового регулювання інформаційно-аналітичної діяльності оперативних підрозділів МВС України.

Література:

1. Ханькевич А. М., Бочковий О. В. Інформаційні технології та забезпечення прав і свобод людини в умовах відкритого суспільства. – Сучасні проблеми правового, економічного та соціального розвитку держави: тези доп. X Міжнародна науково-практична конференція, присвячена 27-й річниці створення Харківського національного університету внутрішніх справ (м. Харків, 19 листопада 2021 р.).– Харків: ХНУВС, 2021.– С. 173-174.

КІБЕРБЕЗПЕКА ПОЛІГРАФОЛОГІЧНИХ ДОСЛІДЖЕНЬ В ПУБЛІЧНІЙ СЛУЖБІ УКРАЇНИ

Здебський Дмитро Володимирович
аспірант 2-го курсу заочної форми навчання докторантури та аспірантури
Одеський державний університет внутрішніх справ
Ісмайлов Карен Юрійович
кандидат юридичних наук, доцент
доцент кафедри кібербезпеки та інформаційного забезпечення
Одеський державний університет внутрішніх справ

Відповідно до Стратегії кібербезпеки України забезпечення кібербезпеки є одним із пріоритетів у системі національної безпеки України. Реалізація зазначеного пріоритету буде здійснюватися шляхом посилення спроможностей національної системи кібербезпеки для протидії кіберзагрозам у сучасному безпековому середовищі [4].

Досвід Національного центру поліграфологічних досліджень США та статистичної розробки, зроблені цією установою, демонструють ефективність використання поліграфів із подальшим підтвердженням отриманих результатів на рівні 95-97% [5, с. 7]. Збільшення кількості поліграфологічних перевірок в секторі публічної служби України є свідченням їх ефективності та визнання в нашій державі. Дану тенденцію актуалізувала перш за все агресія російських окупаційних військ та боротьба з корупцією в Україні. Відповідно до ДСТУ 8692:2016 «Поліграфи. Технічні умови» (далі Стандарт) дослідження із застосуванням поліграфа орієнтовано, насамперед, на захист прав фізичних та юридичних осіб у сфері безпеки їхнього приватного життя, бізнесу або в державній чи правоохоронній діяльності та

для кадрової безпеки [2, с. IV]. З впровадженням поліграфа у публічну службу актуальним постало питання захисту інформації, що отримана за допомогою даного приладу від кіберзагроз, котрі можуть призвести до витоку персональних даних та інформації з обмеженим доступом.

Як визначає зазначений Стандарт – поліграф (детектор брехні) є багатоканальною контрольно-вимірювальною системою, що призначена фіксувати динаміку зміни фізіологічних показників організму людини під час дослідження на визначення його психоемоційного стану у відповідь на пред'явлення за спеціальною методикою певних стимулів і подальше їх відтворення на екрані монітора та збереження й архівування за допомогою пристрою оброблення та відображення інформації, яким можуть бути персональний комп'ютер, планшетний комп'ютер, ноутбук тощо, що їх серійно виробляють, та складається з апаратного комплексу й програмного забезпечення для комп'ютера [2, с. 2]. Під час проведення поліграфологічного дослідження в програмне забезпечення вносяться в електронному вигляді персональні дані суб'єкта опитування із застосуванням поліграфа. Крім того, результат поліграфологічного дослідження фіксуються та зберігається у вигляді поліграм (графічного відображення параметрів фізіологічної активності опитуваного), фіксується час та дата дослідження, а окремі види програмного забезпечення дозволяють здійснювати аудіо- /відеозапис опитування. Потрапляння цих даних до спеціальних служб ворожих до України держав або інших не добропорядних осіб може мати загрози як для державної безпеки так і для охоронюваних державою прав і свобод громадян.

Отже, в ході проведення поліграфологічного дослідження для забезпечення потреб публічної служби України, особливо у військовій сфері та правоохоронній діяльності в умовах збройної агресії російської федерації, кіберзахист даної процедури та отриманих електронних даних має бути безпечним та врегульованим. Однією зі складових поліграфа є комп'ютерне програмне забезпечення. Стандарт визначає програмне забезпечення поліграфа, як сукупність програмних засобів, які забезпечують оброблення цифрових сигналів, що надходять від блока реєстрування та оброблення даних для відображення динаміки їх величини у вигляді діаграм та цифрових показників, а також для їх зберігання та архівування [2, с. 4]. За Стандартом під час роботи з поліграфом має бути дотримано вимоги щодо захисту інформації згідно з ДСТУ ISO/IEC 27001 (міжнародний стандарт з інформаційної безпеки), а в разі необхідності збереження інформації конфіденційної, таємної чи з обмеженим доступом, визначених у ДСТУ 3396.2 (технічний захист інформації, терміни та визначення), й мають бути проведені відповідні роботи та організовано систему технічного захисту інформації згідно з ДСТУ 3396.1 (технічний захист інформації, порядок проведення робіт) [2, с. 6]. В свою чергу, програмне забезпечення поліграфа має відповідати ДСТУ EN 62304 (програмне забезпечення медичних пристроїв) та вимогам інформаційної безпеки для носіїв державної, воєнної та комерційної таємниці [2, с. 7]. Даним Стандартом законодавець передбачив захист персональних даних та інформації з обмеженим доступом поліграфологічних досліджень. Проте, під час проведення практичних поліграфологічних досліджень в секторі публічної служби України даний дотримання правил кібербезпеки не завжди виконується.

Стратегія кібербезпеки України визначає, що російська федерація залишається одним з основних джерел загроз національній та міжнародній кібербезпеці, активно реалізує концепцію інформаційного протиборства, базовану на поєднанні деструктивних дій у кіберпросторі та інформаційно-психологічних операцій, механізми якої активно застосовуються у гібридній війні проти України [4]. Так, у 2015 році один з українських виробників поліграфів розпочав його масове виробництво, проте власного програмного забезпечення даний виріб не мав. Даний поліграф використовувався разом з програмним забезпеченням «Sheriff», яким також комплектуються поліграфи російського виробництва, такі як «Бар'єр», «Кріс» та «Риф» [3]. Правовласником та розробником даного програмного забезпечення в 2007 році було ТОВ «ОРИСЕТ», що мало реєстрацію по вул. Ентузіастів 2-Я, м. Москва, російська федерація, а з 2011 року правонаступницею стало ТОВ «Школа академіка Варламова», розташоване також за адресою у м. Москва, по вул. Біловезька, 41

[1]. Як стверджує виробник, даного поліграфа українського виробництва, його поліграф з 2016 року використовує програмне забезпечення власної розробки. Проте, в ході опитування поліграфологів, що використовують даний комп'ютерний поліграф, програмне забезпечення виробника українських поліграфів є не досконалим, та в ході проведення поліграфологічного дослідження спостерігаються збої в його роботі, що можуть призвести до втрати отриманих даних та анулювання процедури тестування. У зв'язку із зазначеною проблематикою програмного забезпечення виробника, більшість поліграфологів використовують й досі програмне забезпечення російського виробництва. Питання використання російського програмного забезпечення не оминуло так само й поліграфологів публічної служби України. На нашу думку, використання російського програмного забезпечення в поліграфологічних дослідженнях в публічній службі України в умовах збройної агресії російської федерації створює реальну небезпеку витоку службової та конфіденційної інформації. Тим більше використання його в ході проведення поліграфологічних досліджень в секторі безпеки та оборони може призвести до підриву та зниження обороноздатності України та рівня інформаційної безпеки держави.

З метою профілактики та попередження кіберзагроз поліграфологічних досліджень в сфері публічної служби України рекомендуємо:

1. Заборонити використовувати російське програмне забезпечення, що використовується комп'ютерними поліграфами.

2. Унеможливити доступ комп'ютерних систем, що використовуються для поліграфологічних досліджень, до системи Інтернет.

3. Розробити систему шифрування персональних даних суб'єктів опитування із застосуванням поліграфа, для попередження витоку персональних даних.

Відповідно до Стратегії кібербезпеки України прогнозується зростання інтенсивності міждержавного протиборства і розвідувально-підривної діяльності у кіберпросторі шляхом залучення спецслужбами окремих держав, насамперед російської федерації, міжнародних хакерських угруповань для реалізації кібервпливу, при цьому поширюється інструментарій, що передбачає накопичення великих масивів інформації щодо поведінки людини та соціальних груп [4]. Кібербезпека поліграфологічних досліджень, в умовах правового режиму воєнного стану, є одним з пріоритетних напрямків забезпечення обороноздатності держави, дотримання прав суб'єктів опитування із застосуванням поліграфа шляхом забезпечення захисту їх персональних даних, захисту службової та конфіденційної інформації.

Література:

1. Дістало: бізнес-торгівля українськими поліграфами... Застосування поліграфа та спеціальних знань в юридичній практиці: Електронний журнал : веб-сайт. URL: https://expertize-journal.org.ua/all-news/932-distalo-ukrajinskij-poligraf-rubikon-i-obman-peresichnikh-ukrajintsiv-abo-skilki-derzhava-gotova-platiti-za-fejkovi-poligrafi-yaki-ne-vidpovidayut-u-povnomu-obsyazi-vimogam-dstu-8692-201-poligrafi-tekhnichni-umovi (дата звернення: 08.11.2023).

2. ДСТУ 8692:2016. Поліграфи. Технічні умови. Київ : ДП «УкрНДНЦ» Видання офіційне, 2016. 12 с. (Державний стандарт України)

3. Петров Юрій Іванович. Аналітичний огляд комп’ютерних поліграфів та методів обробки біологічних сигналів людини. 2017 рік : Матеріали наук.-тех. конференції. веб-сайт. URL: http://imt.kpi.ua/wp-content/uploads/2017/11/ ANALITYCHNYJ-OGLYAD-KOMPYUTERNYH-POLIGRAFIV-TA-METODIV-OBROBKY-BIOLOGICHNYH-SYGNALIV-LYUDYNY.pdf (дата звернення: 08.11.2023).

4. Про Стратегію кібербезпеки України : Указ Президента України Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року. веб-сайт. URL: https://zakon.rada.gov.ua/laws/show/447/2021#n7 (дата звернення: 08.11.2023).

5. Мотлях О., Корж Є., Куценко Д. Застосування компютерних поліграфів при професійному кадровому відборі до правоохоронних органів України : метод. посіб. Київ, 2019. 144 стор.